MASHaBLE
Mobile Applications of Secret Handshakes over Bluetooth Low-Energy

Yan Michalevsky, Suman Nath, Jie Liu
MOTIVATION

• Private communication
• Anonymous messaging
• Secret communities
• Location-based messaging
• Privacy preserving IoT applications
SECRET COMMUNITIES

- Members want to identify each other
- Do not want to be discovered by anyone not in the community
- Geo-location privacy
- Anonymous messaging and notifications dissemination
“TRUSTED” CENTRAL SERVER

The server becomes a target for attacks
“TRUSTED” CENTRAL SERVER

Internet connectivity is not always available
“TRUSTED” CENTRAL SERVER

Also... GPS and cellular consume a lot of energy
WE WANT TO...

- Avoid interaction with a server
- Use physical proximity
- Minimize energy consumption

Bluetooth Low-Energy (LE) sounds like a promising solution
THE PROBLEM WITH NEGOTIATING TRUST

- Alice is willing to reveal its credentials only to another party with certain clearance (needs to verify Bob’s identity first)
- Bob is also willing to reveal its credentials only to another party with certain clearance (needs to verify Alice’s identity first)
- No party is willing to reveal its credentials and provide a proof of their authenticity first
SECRET HANDSHAKE PROPERTIES

- Parties do not know each other
- They perform a procedure that establishes trust
- If it fails – no information is gained by either party
- If it succeeds – parties reveal membership in a group
  - In addition, they can establish respective roles in that group (cryptographic secret handshakes)
MORE APPLICATIONS

Using iBeacon for headcounting

Car control: Unlock, locate
HEADCOUNTING

• Exposes users to tracking
• Reveals information about the event/gathering
• How do we support private/secret events and provide privacy to attendants?
CAR CONTROL

How do we prevent car and driver tracking?
SECRET HANDSHAKE FROM PAIRINGS

- Based on Balfanz et al. [1]
- If handshake succeeds – both parties have established an authenticated and encrypted communication channel
- If handshake fails – no information is disclosed
- Collusion resistant
  - Corrupted group members cannot collude to perform a handshake of a non-corrupted member
- Compact credentials – important for embedding into small packets
PAIRINGS

We have elements $X \in G_1$ and $Y \in G_2$ where $G_1, G_2$ are algebraic groups.

A pairing $e$ has the following property

$$e(aX, bY) = e(X, Y)^{ab}$$

Where $e(X, Y) \in G_T$
SECRET HANDSHAKE FROM PAIRINGS

Master secret
$t \in \mathbb{Z}_Q$

$(P_A = "p93849", T_A)$

$T_A = t \cdot H(P_A)$

$(P_B = "p12465", T_B)$

$T_B = t \cdot H(P_B)$
SECRET HANDSHAKE FROM PAIRINGS

Master secret
\( t \in \mathbb{Z}_Q \)

\((P_A = "p93849", T_A)\)
\[ T_A = t \cdot H(P_A) \]

\((P_B = "p12465", T_B)\)
\[ T_B = t \cdot H(P_B) \]
SECRET HANDSHAKE FROM PAIRINGS

\[ P_B = "p12465" \]

\[ P_A = "p93849" \]

\[ K_A = e(H(P_B), T_A) = e(H(P_B), H(P_A))^t \]

\[ K_B = e(T_B, H(P_A)) = e(H(P_B), H(P_A))^t \]

\[ Enc_{K_A}(\text{challenge}_A) \]

\[ \text{response}_A, Enc_{K_B}(\text{challenge}_B) \]

\[ \text{response}_B \]
UNLINKABLE HANDSHAKES

- By tracking the pseudonym an attacker can track the user
- Naïve solution:
  - Obtain multiple pseudonyms from master party
  - Use a different pseudonym for each handshake
UNLINKABLE SECRET HANDSHAKE

Master secret
\( t \in \mathbb{Z}_Q \)

\((P_A \in G, T_A = t \cdot P_A)\)

\((P_B \in G, T_B = t \cdot P_B)\)
UNLINKABLE SECRET HANDSHAKE

Master secret
\( t \in \mathbb{Z}_Q \)

\((P_A \in G, T_A = t \cdot P_A)\)

\((P_B \in G, T_B = t \cdot P_B)\)
UNLINKABLE SECRET HANDSHAKE

\[ K_A = e(s \cdot P_B, r \cdot T_A) = e(P_B, P_A)^{rst} \]

\[ K_B = e(s \cdot T_B, r \cdot P_A) = e(P_B, P_A)^{rst} \]
SOME DETAILS

- Need to hash arbitrary strings onto $G_2$
  - Supported by Type 1 or Type 3 pairings

- Group element sizes
  - 128-bit security: 256-bit group element size = 32 bytes
  - 80-bit security: 160-bit element size = 20 bytes
TRACKING PREVENTION

- *Random device address* for Bluetooth source address field
  - Set dynamically and changed across different connections
BLUETOOTH LE ADVERTISEMENTS

- Scanning is supported by
  - Windows phone
  - Android
  - iOS

- Publishing advertisements is supported on
  - Windows phone 10
  - Possibly future Android phone versions
  - Kits such as Cypress and Dialog
PAIRING METHODS

- Just Works
  - Basically no MITM protection during pairing phase
- Passkey entry
  - Proven to be quite weak [7]
- Out-of-Band (OOB) – credentials provided by some other method
PROPOSAL: NEW PAIRING MODE

A

B

Selection of pairing method

Pairing Confirm (Mconfirm) - $P_M$

Pairing Confirm (Sconfirm) - $P_S, Challenge_S$

Parties calculate shared key using pairings – serves as STK

Pairing Random (Mrand) – $Response_S, Challenge_M$

Pairing Random (Srand) $Response_M$

128-bit only!!!
BLUETOOTH LE ADVERTISEMENTS

- Bluetooth LE supports broadcasting advertisements
- Clients can scan and filter advertisements of specific types
- A little custom data can be squeezed in – 32 bytes
  - On Windows BTLE stack we currently can only control the Manufacturer Specific Data (AD type 0xFF) – 20 bytes
CHOICE OF PLATFORM

- Easy implementation of pairings
  - JPBC – Java port of Stanford PBC library
- iOS and Android did not support publishing
  - Android exposed the API but did not support advertising in practice
- Windows Phone
  - Supports scanning and advertising
  - Possible to scan and advertise at the same time
IMPLEMENTATION

▪ Windows Phone OS 10
▪ Failed attempt: porting JPBC to .NET
▪ Pairings and group operations using Stanford PBC library
  ▪ Ported to ARM + .NET wrapper (PbcProxy)
  ▪ Used MPIR library (Multi-Precision Integers and Rationals, compatible with GMP)
  ▪ Adapted random number generation
▪ Communication between two phones is based on alternation between advertising and scanning
EVALUATION: FUNCTIONALITY

- Two mobile phones running our app and performing handshakes
- Experiment duration: 8296 sec = 2 hours 18 sec
- 1 handshake every 8 seconds
- Total 1068 handshakes
- 1025 succeeded, 43 failed. Success rate: 96%
EVALUATION: ENERGY CONSUMPTION

• Nokia Lumia 920 running Windows Phone OS
• Starting with 100% charge, Wi-Fi and GPS off
• Modes:
  • Baseline
  • Advertising
  • Scanning
  • Advertising + handshake
  • Scanning + handshake
• Experiment duration: 3 hours
EVALUATION: ENERGY CONSUMPTION

Enables >12 hours of operation
COMMUNICATION OVERHEAD

- Advertisement packet: 47 bytes
- Each party sends 2 packets: 94 bytes
FUTURE WORK

▪ Pairing preprocessing
  ▪ For each handshake using the same credentials preprocessing can be applied
  ▪ Supported by PBC library

▪ Use BLE specific identifiers as handshake pseudonyms
  ▪ Set a custom source device address
  ▪ Would provide additional usable space for longer pseudonyms

▪ More Windows Universal applications using PbcProxy
THANKS

Questions?
RELATED WORK

- Automatic Trust Negotiation (ATN)
- Attribute-Based Encryption (ABE)
  - Decryption is possible if party is certified as possessing certain attributes by an authority
- Secret handshakes [1]
  - Each party receives a certificate from a central authority
- Hidden credentials [2]
  - Protect the messages using policies that require possession of multiple credentials
- Oblivious Signature-Based Envelope (OSBE) [8]
  - Allows certificates issued by different authorities
- Secret handshakes from CA-oblivious encryption [9]
- Unlinkable secret handshakes and key-private group key management schemes [10]
REFERENCES

1. Secret handshakes from pairing-based key agreements [Balfanz et al. 2003]
2. Hidden credentials [Holt et al. 2003]
3. Authenticated Identity-Based Encryption [Lynn 2002]
4. How tracking customers in stores will soon be norm
5. How retail stores track you using your smartphone (and how to stop it)
6. Apple is quietly making its move to own in-store digital tracking
8. Oblivious Signature-Based Envelope [Li et al. 2003]
9. Secret handshakes from CA-oblivious encryption [Casteluccia et al. 2004]
10. Unlinkable secret handshakes and key-private group key management schemes [Jarecki et al. 2007]